(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 42 43 851 A 1**

(51) Int. Cl.[5]:
G 06 F 15/21
G 07 F 7/08
G 06 K 19/07
B 42 D 15/10

(21) Aktenzeichen: P 42 43 851.9
(22) Anmeldetag: 23. 12. 92
(43) Offenlegungstag: 30. 6. 94

(71) Anmelder:
Deutsche Bundespost Telekom, 53175 Bonn, DE; International Business Machines Corp., Armonk, N.Y., US; Orga Datentechnik GmbH, 4790 Paderborn, DE; GAD Gesellschaft für automatische Datenverarbeitung eG, 4400 Münster, DE

(74) Vertreter:
Herzog, F., Dipl.-Ing., Pat.-Anw., 71155 Altdorf

(72) Erfinder:
Endler, Reinhard, 8501 Roßtal, DE; Westphal, Reinhard, 8501 Roßtal, DE; Hartleif, Siegfried, 8114 Groß-Umstadt, DE; Niehaus, Herbert, 48165 Münster, DE; Schäfer, Peter, 48159 Münster, DE; Mergemeier, Detlev, 58239 Schwerte, DE; Hovemeyer, Dieter, 33100 Paderborn, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE	42 18 923 A1
DE	41 19 924 A1
DE	40 13 147 A1
DE	38 44 033 A1
DE	34 12 663 A1
US	48 39 504

(54) Verfahren zum Transferieren von Buchgeldbeträgen auf und von Chipkarten

(57) Bei bekannten Verfahren wird davon ausgegangen, daß debitorische und kreditorische Börsenfunktionen unabhängig voneinander arbeiten. Der erfindungsgemäßen Lösung liegt die Aufgabe zugrunde, die Vorteile der kreditorischen Börse mit den Vorteilen der debitorischen Börse zu vereinen. Erfindungsgemäß werden überschreibbare Speicherplätze einer Chipkarte in einen Speicherplatz für kreditorische Börsenfunktionen und mindestens einen Speicherplatz für debitorische Börsenfunktionen aufgeteilt. Über das Applikationsprogramm der Chipkarte wird in Verbindung mit dem Programm eines Autorisierungssystems ein Buchgeldbetrag aus der kreditorischen Börse, einmalig oder mehrfach hintereinander, in die debitorische Börse transferiert. Durch die erfindungsgemäße Lösung ist der Dienstenutzer in der Lage, mittels nur einer multifunktionalen Chipkarte, jederzeit aus dem ihm im Rahmen der kreditorischen Börse gewährten Kredit die debitorische Börse der Chipkarte aufzufüllen.

DE 42 43 851 A1

E

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 05. 94 408 026/145

Beschreibung

Die Erfindung betrifft ein Verfahren zum Transferieren von Buchgeldbeträgen auf und von gesicherten Chipkarten, die einen Identifizierungscode enthalten, der in Verbindung mit einem autorisierten Schlüssel in einem Autorisierungssystem aktiviert wird.

Einfache spezielle Börsenlösungen auf Chipkarten sind verschiedentlich im Einsatz. Auf internationaler Ebene werden zur Zeit sowohl debitorische als auch kreditorische Börsen spezifiziert (ETSI D/EN/TE 090114, Terminal Equipment (TE); Requirements for IC cards and terminals for telecommunication use, Part 4 — Payment methods, Version: 4, Date: 7 February 1992 und CEN/TC224/WG10; Intersector Electronic purse, DRAFT: prEN xxxxx-1, Date: 21.02.92).

Mit der kreditorischen Börsenfunktion wird dem Dienstenutzer ein Kreditrahmen eingeräumt, den er für unterschiedliche, meist höherwertige Bezahlvorgänge nutzen kann.

Mit der debitorischen Börsenfunktion verfügt der Dienstenutzer über ein "elektronisches Portemonnaie", mit dem er zumeist niedrigpreisige Bezahlvorgänge tätigen kann, wie z. B. telefonieren, Fahrscheine kaufen, Parkgebühren bezahlen etc. Die Abwicklung kann über eine oder mehrere debitorische Börsen für unterschiedliche Diensteanbieter erfolgen. Mit der debitorischen Börse hat der Dienstenutzer den Vorteil

— der schnellen Abwicklung von Zahlungsvorgängen,
— der Anonymität der Zahlungsvorgänge und
— des unmittelbaren Überblickes über seine Ausgaben.

Eine debitorische Börse mit oben beschriebenen Vorteilen weist dagegen nicht den Sicherheitsstandard einer kreditorischen Börsenfunktion auf. So ist z. B. ein PIN-Handling oder eine Online-Authentifizierung an Billigterminals, wie z. B. an einem Fahrkartenautomaten im Bus, entweder sehr zeitaufwendig oder gar nicht möglich. Eine debitorische Börse darf also im Interesse d Benutzers keine größeren Buchgeldbeträge beinhalten und muß dementsprechend oft neu aufgeladen werden.

Bei allen bekannten Lösungen wird immer davon ausgegangen, daß debitorische oder kreditorische Börsenfunktionen unabhängig voneinander arbeiten.

Der Erfindung liegt die Aufgabe zugrunde, die Vorteile der kreditorischen Börse mit den Vorteilen der debitorischen Börse zu vereinen.

Erfindungsgemäß werden die überschreibbaren Speicherplätze einer Chipkarte in mindestens einen Speicherplatz, der für kreditorische Börsenfunktionen eingerichtet ist und in mindestens einen Speicherplatz, der für debitorische Börsenfunktionen eingerichtet ist, aufgeteilt. Über das Applikationsprogramm der Chipkarte wird in Verbindung mit dem Programm eines Autorisierungssystems ein Buchgeldbetrag aus der kreditorischen Börse, einmalig oder mehrfach hintereinander, in die debitorische Börse transferiert. Der Transfervorgang kann sowohl über ein Autorisierungssystem als auch kartenintern erfolgen. Darüber hinaus ist die debitorische Börse so offen angelegt, daß sie jederzeit auch direkt aus einem Autorisierungssystem geladen werden kann, wie z. B. aus einem Geldautomaten, einem Bankenterminal oder einem Kartentelefon.

Beim Transfer eines Geldbetrages über ein Autorisierungssystem wird zunächst der umzuladende Buchgeldbetrag aus dem kreditorischen Börsenfeld in das Autorisierungssystem geladen. Die Chipkarte gibt dazu über ihr Applikationsprogramm gleichzeitig eine kryptographisch gesicherte Quittung an das Autorisierungssystem ab.

Anschließend wird der gleiche Betrag vom Autorisierungssystem in das debitorische Börsenfeld der Chipkarte geladen. Dieser Ladevorgang wird ebenfalls kryptographisch abgesichert quittiert. Das Autorisierungssystem erzeugt mit beiden Quittungen einen Buchungsdatensatz, der vom Diensteanbieter der debitorischen Börse beim Diensteanbieter der kreditorischen Börse eingereicht wird. Der Diensteanbieter der kreditorischen Börse authentifiziert die Quittungen des Buchungsdatensatzes. Der umgebuchte Betrag wird dann dem Betreiber der debitorischen Börse gutgeschrieben. Das Konto des Dienstenutzers wird dementsprechend belastet.

Beim karteninternen Transferieren eines Buchgeldbetrages wird der Transfer vom Autorisierungssystem in Gang gesetzt und läuft dann kartenintern über das Applikationsprogramm der Chipkarte ab. Die Chipkarte erzeugt über ihr Applikationsprogramm einen kryptographisch gesicherten Datensatz, der vom Diensteanbieter der debitorischen Börse beim Diensteanbieter der kreditorischen Börse zur Verrechnung eingereicht wird. Der transferierte Betrag wird vom Diensteanbieter der kreditorischen Börse authentifiziert und dem Diensteanbieter der debitorischen Börse gutgeschrieben. Das Konto des Dienstenutzers wird entsprechend belastet.

Anhand eines Beispiels

— für den Transfer eines Buchgeldbetrages über ein Autorisierungssystem und
— für das karteninterne Transferieren eines Buchgeldbetrages in Verbindung mit einem Autorisierungssystem wird die erfindungsgemäße Lösung näher erläutert.

Beim Transferieren eines Buchgeldbetrages über ein Autorisierungssystem wird nach dem Eingeben der Chipkarte in ein Endgerät, wie beispielsweise ein Kartentelefon, dem Dienstenutzer über ein Terminal der aktuelle Stand seiner debitorischen und kreditorischen Börse angezeigt. Parallel dazu findet sowohl eine Authentifikation der Chipkarte gegenüber dem Autorisierungssystem, als auch eine Authentifikation des Autorisierungssystems gegenüber der Chipkarte durch geeignete kryptographische Verfahren statt.

Wenn der Dienstenutzer sich zum Auffüllen seiner debitorischen Börse entschließt, wird durch das Auslösen eines dementsprechenden Befehls durch den Dienstenutzer der Umbuchungsvorgang ausgelöst. Dabei werden zunächst weitere Daten der debitorischen Börse der Chipkarte über das Endgerät an das Autorisierungssystem übertragen.

Anhand des Programms des Autorisierungssystem wird überprüft, ob das Verfallsdatum der debitorischen Börse abgelaufen ist, ob die Seriennummer in einer Sperrliste steht und ob mit dem Aufladevorgang das Limit des Geldbetrages für die debitorische Börse überschritten wird. Bei erfolgreicher Prüfung über das Programm des Autorisierungssystems erfolgt ein Auslesen weiterer Daten der kreditorischen Börse der Chipkarte.

Über das Programm des Autorisierungssystems wird ebenfalls geprüft, ob das Verfallsdatum der kreditorischen Börse abgelaufen ist, ob die Seriennummer in

einer Sperrliste steht und ob der Kreditrahmen bei Abbuchung der gewünschten Summe gewahrt bleibt.

Anschließend wird der Dienstenutzer durch das Programm des Autorisierungssystems über das Endgerät zur Eingabe seiner persönlichen Geheimzahl PIN aufgefordert. Durch Eingabe der PIN und bei erfolgreicher Überprüfung durch die Chipkarte erfolgt über den kryptographisch gesicherten Abbuchungsbefehl, der vom Autorisierungssystem über das Endgerät zur Chipkarte übertragen wird, die Abbuchung des gewünschten Buchgeldbetrages aus der kreditorischen Börse.

Als Quittung über die Abbuchung des Buchgeldbetrages von der kreditorischen Börse wird mittels des Applikationsprogrammes der Chipkarte über das Endgerät ein kryptographisch gesicherter Buchungsdatensatz erstellt, der vom Dienstebetreiber der debitorischen Börse zur Verrechnung beim Diensteanbieter der kreditorischen Börse eingereicht wird. Gleichzeitig wird ein Message-Authentifikations-Code MAC übertragen. Der MAC wird gebildet, indem die Klartextdaten des Buchungsdatensatzes mit einem in der Chipkarte vorhandenen Schlüssel des Dienstebetreibers der kreditorischen Börse verschlüsselt werden. Mit dem MAC überprüft der Dienstebetreiber der kreditorischen Börse die Echtheit des Buchungsdatensatzes, indem er den MAC entschlüsselt und die Daten mit den Klartexten im Buchungsdatensatz vergleicht.

Nach Prüfung des Buchungsdatensatzes wird der aus der kreditorischen Börse abgebuchte Buchgeldbetrag (zuzüglich MAC) ebenfalls kryptographisch gesichert, vom Autorisierungssystem über das Endgerät in die debitorische Börse geladen.

Die Quittung über den in die debitorische Börse der Chipkarte geladenen Buchgeldbetrag zuzüglich MAC erfolgt wiederum in Form einer MAC-gesicherten Bestätigung, genannt MAC'. Sie wird kryptographisch gesichert über das Endgerät zum Autorisierungssystem übertragen.

Mit dem MAC' überprüft der Dienstebetreiber der kreditorischen Börse, ob dem Dienstenutzer auch tatsächlich die Dienstleistung, nämlich das Laden des aus der kreditorischen Börse entnommenen Buchgeldbetrages in die debitorische Börse, erbracht wurde.

Patentansprüche

1. Verfahren zum Transferieren von Buchgeldbeträgen auf und von Chipkarten mit mindestens zwei überschreibbaren Speicherplätzen, unter Verwendung von Diensteanbieter-Endgeräten, die mit einem Autorisierungssystem verbindbar sind, wobei bekannte Verfahren, sowohl für die Buchung als auch für die kryptographisch abgesicherte Erstellung von Buchungsquittungen zum Einsatz kommen, **dadurch gekennzeichnet**, daß die überschreibbaren Speicherplätze der Chipkarte in einen kreditorischen und mindestens einen debitorischen Speicherplatz aufgeteilt werden, wobei über das Applikationsprogramm der Chipkarte in Verbindung mit dem Programm eines Autorisierungssystems ein in einem vorgegebenen Kreditrahmen beliebig oft wiederholbares Umbuchen von Buchgeldbeträgen aus dem Speicherbereich für kreditorische Börsenfunktion in den Speicherbereich für debitorische Börsenfunktion realisiert wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß nach dem Eingeben der Chipkarte in ein Endgerät eines Dienstebetreibers dem Dienstenutzer der aktuelle Stand der debitorischen und kreditorischen Börse angezeigt wird,

— daß parallel zur Anzeige der Beträge eine Authentifikation der Chipkarte gegenüber dem Autorisierungssystem, als auch eine Authentifikation des Autorisierungssystems gegenüber der Chipkarte durch geeignete kryptographische Verfahren stattfindet,

— daß nach Auslösen des Umbuchungsvorganges durch den Dienstenutzer zum Auffüllen der debitorischen Börse zunächst weitere Daten der debitorischen Börse der Chipkarte an das mit dem Endgerät ansteuerbare Autorisierungssystem übertragen werden,

— daß anhand des Programms des Autorisierungssystems überprüft wird, ob das Verfallsdatum der debitorischen Börse abgelaufen ist, ob die Seriennummer in einer Sperrliste steht und ob mit dem Aufladevorgang das Limit des Buchgeldbetrages für die debitorische Börse überschritten wird,

— daß bei erfolgreicher Prüfung über das Programm des Autorisierungssystems ein Auslesen weiterer Daten der kreditorischen Börse der Chipkarte erfolgt,

— daß über das Programm des Autorisierungssystems geprüft wird, ob das Verfallsdatum der kreditorischen Börse abgelaufen ist, ob die Seriennummer in einer Sperrliste steht und ob der Kreditrahmen bei Abbuchung der gewünschten Summe gewahrt bleibt,

— daß der Dienstenutzer durch das Programm des Autorisierungssystems über das Endgerät zur Eingabe seiner persönlichen Geheimzahl PIN aufgefordert wird,

— daß nach Eingabe der PIN und bei erfolgreicher Überprüfung durch die Chipkarte über den kryptographisch gesicherten Abbuchungsbefehl, der vom Autorisierungssystem zum Endgerät übertragen wird, die Abbuchung des gewünschten Buchgeldbetrages aus der kreditorischen Börse erfolgt,

— daß als Quittung über die erfolgte Abbuchung des Buchgeldbetrages von der kreditorischen Börse, mittels des Applikationsprogrammes der Chipkarte, über das Endgerät ein Buchungsdatensatz und ein Message-Authentifikations- Code MAC erzeugt und zum Autorisierungssystem übertragen werden,

— daß nach Prüfung des Buchungsdatensatzes in Verbindung mit dem MAC der aus der kreditorischen Börse abgebuchte Buchgeldbetrag, ebenfalls kryptographisch gesichert, vom Autorisierungssystem über das Endgerät in die debitorische Börse geladen wird,

— daß als Quittung über den in die debitorische Börse der Chipkarte geladenen Buchgeldbetrag zuzüglich MAC wiederum eine MAC-gesicherte Bestätigung, genannt MAC', kryptographisch gesichert über das Endgerät zum Autorisierungssystem übertragen wird, und

— daß MAC und MAC' mit Schlüsseln des Dienstebetreibers der kreditorischen Börse gebildet werden.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet,

— daß nach dem Eingeben der Chipkarte in ein Endgerät eines Dienstebetreibers dem

Dienstebenutzer der aktuelle Stand der debitorischen und kreditorischen Börse angezeigt wird,

— daß parallel zur Anzeige der Beträge eine Authentifikation der Chipkarte gegenüber dem Autorisierungssystem, als auch eine Authentifikation des Autorisierungssystems gegenüber der Chipkarte durch geeignete kryptographische Verfahren stattfindet,

— daß nach Auslösen eines Umbuchungsvorganges durch den Dienstenutzer zum Auffüllen der debitorischen Börse zunächst weitere Daten der debitorischen Börse der Chipkarte an das mit dem Endgerät ansteuerbare Autorisierungssystem übertragen werden,

— daß anhand des Programms des Autorisierungssystems überprüft wird, ob das Verfallsdatum der debitorischen Börse abgelaufen ist, ob die Seriennummer in einer Sperrliste steht und ob mit dem Aufladevorgang das Limit des Buchgeldbetrages für die debitorische Börse überschritten wird,

— daß bei erfolgreicher Prüfung über das Programm des Autorisierungssystems ein Auslesen weiterer Daten der kreditorischen Börse der Chipkarte erfolgt,

— daß über das Programm des Autorisierungssystems geprüft wird, ob das Verfallsdatum der kreditorischen Börse abgelaufen ist, ob die Seriennummer in einer Sperrliste steht und ob der Kreditrahmen bei Abbuchung der gewünschten Summe gewahrt bleibt,

— daß der Dienstenutzer durch das Programm des Autorisierungssystems über das Endgerät zur Eingabe seiner persönlichen Geheimzahl PIN aufgefordert wird,

— daß durch Eingabe der PIN und bei erfolgreicher Überprüfung durch die Chipkarte über den kryptographisch gesicherten Umbuchungsbefehl, der vom Autorisierungssystem über das Endgerät zur Chipkarte übertragen wird, die Umbuchung des gewünschten Buchgeldbetrages aus der kreditorischen in die debitorischen Börse erfolgt,

— daß als Quittung über den von der kreditorischen Börse in die debitorische Börse umgebuchten Buchgeldbetrag wiederum eine MAC-gesicherte Bestätigung kryptographisch abgesichert über das Endgerät zum Autorisierungssystem übertragen wird.

— daß der MAC mit dem Schlüssel des Dienstebetreibers der kreditorischen Börse gebildet wird, so daß dieser eine Validierung des Umbuchungsvorganges vornehmen kann.